

University of Wollongong

Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information
Sciences

1980

Complex weighing matrices and orthogonal designs

Jennifer Seberry

University of Wollongong, jennie@uow.edu.au

Albert L. Whiteman

Follow this and additional works at: <https://ro.uow.edu.au/infopapers>



Part of the [Physical Sciences and Mathematics Commons](#)

Recommended Citation

Seberry, Jennifer and Whiteman, Albert L.: Complex weighing matrices and orthogonal designs 1980.
<https://ro.uow.edu.au/infopapers/997>

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Complex weighing matrices and orthogonal designs

Abstract

Galois fields $GF(q^2)$ are used to obtain a new infinite family of complex weighing matrices. $CW(q+1, q)$, $q \equiv 1 \pmod{8}$, and type P = $[R - S S^* - R^*]$ where R and S are symmetric complex circulants. These matrices are used to construct orthogonal designs. Some unsolved cases of Geramita and Geramita are also settled.

Disciplines

Physical Sciences and Mathematics

Publication Details

Seberry, J and Whiteman, AL, Complex weighing matrices and orthogonal designs, *Ars Combinatoria*, 9, 1980, 149-162.

COMPLEX WEIGHING MATRICES AND ORTHOGONAL DESIGNS.

Jennifer Seberry and Albert Leon Whiteman

Abstract

Galois fields $GF(q^2)$ are used to obtain a new infinite family of complex weighing matrices $CW(q+1, q)$, $q \equiv 1 \pmod{8}$, and type

$$P = \begin{bmatrix} R & -S \\ S^* & -R^* \end{bmatrix}$$

where R and S are symmetric complex circulants.

These matrices are used to construct orthogonal designs. Some unsolved cases of Geramita and Geramita are also settled.

1. Introduction.

An orthogonal design of order n and type (s_1, \dots, s_u) on the commuting variables x_1, \dots, x_u is an $n \times n$ matrix X with entries chosen from the set $\{0, \pm x_1, \dots, \pm x_u\}$ such that

$$XX^T = \left(\sum_{i=1}^u s_i x_i^2 \right) I_n.$$

Such generically orthogonal matrices have played a significant role in the construction of Hadamard matrices (see eg. the book [5]) and they have already been extensively used in the study of weighing matrices $W(n, k) = W$ which have entries $0, 1, -1$ and satisfy

$$WW^T = kI_n.$$

These have been studied extensively [1, 2, 5, 8, 9, 12, 13] and one of us (Seberry) has conjectured [13] that for $n \equiv 0 \pmod{4}$ there is a weighing matrix of order n and weight k for every $k \leq n$.

Later the notion of a complex Hadamard matrix, i.e., an $n \times n$ matrix C whose entries are chosen from $\{\pm 1, \pm i\}$ and satisfying $CC^* = nI_n$ ($*$ = complex conjugate) were studied in order to obtain new Hadamard

matrices (see [11, p. 347-353]).

Recently the study of *complex orthogonal designs (cod)* of order n and type (s_1, \dots, s_u) (s_i positive integers) which is an $n \times n$ matrix X with entries chosen from $\{0, i_1 x_1, \dots, i_u x_u\}$, where i_j is a fourth root of 1 and x_1, \dots, x_u are real variables, satisfying

$$XX^* = \left(\sum_{j=1}^u s_j x_j^2 \right) I_n$$

was commenced in [4].

We note that if $\{i_1, \dots, i_u\} = \{+1\}$ we have an orthogonal design as

previously defined. If $\sum_{j=1}^u s_j = n$ and $\{i_1, \dots, i_u\} = \{+1, +i | i^2 = -1\}$

we have a complex Hadamard matrix but if $\{i_1, \dots, i_u\} = \{+1\}$ we have a Hadamard matrix.

If $\sum_{j=1}^u s_j = k$, $k \leq n$ we have a *complex weighing matrix* $CW(n, k)$ or

weighing matrix according as $\{i_1, \dots, i_u\} = \{+1, +i\}$ or $\{+1\}$. Complex weighing matrices have been studied with great interest lately [2, 10] because of their connection with combinatorial designs. The notation $CW(n, k, z_4)$ is sometimes used to denote the elements are from the cyclic group z_4 and distinguish it from $CW(n, k, f_2 \times f_2)$.

2. A Preliminary Lemma.

Let $GF(q^2)$ denote a finite field of q^2 elements where $q = p^r$ is an odd prime power. Let τ denote a generator of the cyclic group of non-zero elements of $GF(q^2)$. Put $\gamma = \tau^{(q+1)/2}$ and $g = \gamma^2$. Then g is a generator of the cyclic group of non-zero elements of a finite field $GF(q)$ of order q . It follows that $\gamma^q = -\gamma$. We also have $GF(q^2) = \{a\gamma + b; a, b \in GF(q)\}$.

For arbitrary $\xi \in GF(q^2)$ define

$$\text{tr}(\xi) = \xi + \xi^q \quad (1)$$

so that $\text{tr}(\xi) \in GF(q)$. It follows at once from this definition that

$$\text{tr}(\tau^k) = \tau^{(q+1)k} \text{tr}(\tau^{-k}), \quad (2)$$

for any integer κ . For $\xi \in GF(q^2)$, $\xi \neq 0$, let $\text{ind}(\xi)$ be the least non-negative integer t such that $\tau^t = \xi$. Let β denote a primitive eighth root of unity. Then

$$\chi(\xi) = \begin{cases} \beta^{\text{ind}(\xi)} & (\xi \neq 0) \\ 0 & (\xi = 0), \end{cases} \quad (3)$$

defines an eighth power character χ of $GF(q^2)$. For $a \in GF(q)$, $a \neq 0$, put $q^j = a$. Then (3) implies that $\chi(a) = \beta^{(q+1)j}$.

Suppose henceforth that $q \equiv 1 \pmod{8}$ so that $\chi(a) = i^j$. This means that the restriction of χ to $GF(q)$ reduces the character $\chi(a)$ to a fourth power character over $GF(q)$. Thus $\chi(a) = 1, -1, i$ or $-i$ according as $j \equiv 0, 2, 1$ or $3 \pmod{4}$. Accordingly we deduce from (2) that

$$\chi(\text{tr}(\tau^\kappa)) \overline{\chi(\text{tr}(\tau^{-\kappa}))} = i^\kappa \quad (\text{tr}(\tau^\kappa) \neq 0), \quad (4)$$

where $\overline{\chi(\xi)}$ is the complex conjugate of $\chi(\xi)$.

It will later be convenient to introduce $\theta = \tau^{q-1}$, an element of $GF(q^2)$ of multiplicative order $q+1$. Since $\text{tr}(\tau^\kappa) = \tau^\kappa(\theta^\kappa + 1)$ we have

$$\chi(\text{tr}(\tau^\kappa)) = \beta^\kappa \chi(\theta^\kappa + 1). \quad (5)$$

The proof of Theorem 1 in the next section is based upon the following lemma.

LEMMA 1. If r is a non-negative integer, then

$$\sum_{\kappa=0}^q \chi(\text{tr}(\tau^\kappa)) \overline{\chi(\text{tr}(\tau^{\kappa+r}))} = \begin{cases} (-i)^j q & (q+1 \mid r), \\ 0 & (q+1 \nmid r), \end{cases} \quad (6)$$

where, in the first case, $r = j(q+1)$.

Proof. For fixed $\eta \in GF(q^2)$ put $\eta = c\gamma + d$, $c, d \in GF(q)$. Then $\eta \in GF(q)$ if $c = 0$ and $\eta \notin GF(q)$ if $c \neq 0$. We first show that

$$\sum_{\xi} \chi(\text{tr}(\xi)) \overline{\chi(\text{tr}(\eta\xi))} = \begin{cases} \overline{\chi(d)} q(q-1) & (c = 0), \\ 0 & (c \neq 0). \end{cases} \quad (7)$$

where the summation extends over all $\xi \in GF(q^2)$. Put $\xi = a\gamma + b$, $a, b \in GF(q)$. By (1) we have $\text{tr}(\xi) = 2b$ and $\text{tr}(\eta\xi) = 2(gac + bd)$. Therefore

$$\sum_{\xi} \chi(\text{tr}(\xi)) \overline{\chi(\text{tr}(\eta\xi))} = \sum_b \chi(b) \sum_{\xi} \chi(gac + bd),$$

and (7) follows at once.

For $\eta \neq 0$ we may put $\eta = \tau^r$, $0 \leq r \leq q^2 - 2$, so that $c = 0$ if $q+1 \mid r$ and $c \neq 0$ if $q+1 \nmid r$. If $c = 0$ put $r = j(q+1)$ then we get $\chi(d) = i^j$. The sum in (7) now becomes

$$\sum_{\kappa=0}^{q^2-2} \chi(\text{tr}(\tau^\kappa)) \overline{\chi(\text{tr}(\tau^{\kappa+r}))} = \sum_{h=0}^{q-2} \sum_{\kappa=h(q+1)}^{h(q+1)+q} \chi(\text{tr}(\tau^\kappa)) \overline{\chi(\text{tr}(\tau^{\kappa+r}))}.$$

In view of (7), the double sum on the right has the value 0 if $q+1 \nmid r$. Since $\chi(\text{tr}(\tau^{\kappa+q+1})) = i \chi(\text{tr}(\tau^\kappa))$, the value of the inner sum is the same for each h . In particular, for $h = 0$ we obtain the result stated in the lemma.

3. The main theorem.

The idea of associating with a circulant matrix A of order n the polynomial

$$\psi(\zeta) = a_0 + a_1 \zeta + \dots + a_{n-1} \zeta^{n-1},$$

where the coefficients a_0, a_1, \dots, a_{n-1} comprise the top row of A and ζ is an n th root of unity has been exploited by Williamson [14]. One may also associate with $\psi(\zeta)$ a finite Parseval relation. If the coefficients of $\psi(\zeta)$ are complex numbers, this relation is given for fixed r by

$$\sum_{i=0}^{n-1} a_i \overline{a_{i+r}} = \frac{1}{n} \sum_{j=0}^{n-1} |\psi(\zeta^j)|^2 \zeta^{jr}, \quad (8)$$

where $\overline{a_{i+r}}$ is the conjugate of a_{i+r} and $\zeta = \exp(2\pi i/n)$.

We shall employ the finite Parseval relation to prove the following theorem.

THEOREM 1. Let q be a prime power $\equiv 1 \pmod{8}$ and put $n = (q+1)/2$. Let τ be a primitive element of $GF(q^2)$. Put $\tau^k = a\gamma + b$, $a, b \in GF(q)$, and define

$$a_k = \chi(a), \quad b_k = \chi(b). \quad (9)$$

Then the sums

$$f(\zeta) = \sum_{i=0}^{n-1} a_{8i} \zeta^i, \quad g(\zeta) = \sum_{i=0}^{n-1} b_{8i} \zeta^i \quad (10)$$

satisfy the identity

$$|f(\zeta)|^2 + |g(\zeta)|^2 = q \quad (11)$$

for each n th root of unity including $\zeta = 1$.

Note that (with the exception of $a_0 = 0$) the coefficients a_{8i}, b_{8i} are $\pm 1, \pm i$. When q is a prime $\equiv 1 \pmod{8}$ and $\zeta = 1$, the identity (11) reduces to the classical result that every prime $\equiv 1 \pmod{8}$ is representable in the form $c^2 + 2d^2$ with integral values of c and d . This is true for the following reason. In the proof of the corollary of Theorem 1 we show that $f(1)$ reduces to $d(1+i)$. Moreover, $g(1)$ is actually real and reduces to c with $c \equiv 1 \pmod{4}$. Consequently $|f(1)|^2 + |g(1)|^2 = c^2 + 2d^2 = q$.

Proof of Theorem 1. Since τ is a primitive element of $GF(q^2)$ the integer $k = (q+1)/2 = n$ is the only value of k in the interval $0 \leq k \leq q$ for which $\text{tr}(\tau^k) = 0$. Since $\tau^n = \gamma$, the numbers a_k, b_k in (9) satisfy the periodicity relation

$$\begin{aligned} a_{k+2jn} &= i^j a_k, & b_{k+2jn} &= i^j b_k, \\ a_{k+(2j+1)n} &= i^j b_k, & b_{k+(2j+1)n} &= i^{j+1} a_k. \end{aligned} \quad (12)$$

From (4) we deduce the second of the two relations

$$a_k = i^k a_{8n-k}, \quad b_k = i^k b_{8n-k}.$$

The first relation follows from the second upon replacing k by $k+n$ and then applying the last relation in (12). For $k = 8r$ we get in particular

$$a_{8r} = a_{8(n-r)}, \quad b_{8r} = b_{8(n-r)} \quad (r = 0, 1, \dots, n-1) \quad (13)$$

Let us now apply the finite Parseval relation (8) to the two sums in (10). We obtain

$$\sum_{i=0}^{n-1} (a_{8i} \bar{a}_{8i+8r} + b_{8i} \bar{b}_{8i+8r}) = \frac{1}{n} \sum_{j=0}^{n-1} (|f(\zeta^j)|^2 + |g(\zeta^j)|^2) \zeta^{jr}, \quad (14)$$

where $\zeta = \exp(2\pi i/n)$.

Let $8i \equiv s \pmod{q+1}$, s even, $0 \leq s < q+1$, and $8i+n \equiv t \pmod{q+1}$, t odd, $1 \leq t < q+1$. As i runs over the integers from 0 to $n-1$, the numbers s run over the even integers from 0 to $q-1$ in some order, and the numbers t run over the odd integers from 1 to q in some order. Making use of the third relation in (12) we find that the sum in the left member of (14) reduces to

$$\begin{aligned} & \sum_{i=0}^{n-1} b_{8i} \bar{b}_{8i+8r} + \sum_{i=0}^{n-1} b_{8i+n} \bar{b}_{8i+n+8r} \\ &= \sum_{j=0}^{n-1} b_{2j} \bar{b}_{2j+8r} + \sum_{j=0}^{n-1} b_{2j+1} \bar{b}_{2j+1+8r} = \sum_{k=0}^q b_k \bar{b}_{k+8r} \end{aligned} \quad (15)$$

We next employ Lemma 1. We denote the sum in (6) by $F(r)$. The sum in the last member of (15) is equal to $F(8r)$. Combining (14) and (15) we get

$$F(8r) = \frac{1}{n} \sum_{j=0}^{n-1} (|f(\zeta^j)|^2 + |g(\zeta^j)|^2) \zeta^{jr}. \quad (16)$$

The inverted form of (16) is

$$|f(\zeta^j)|^2 + |g(\zeta^j)|^2 = \sum_{r=0}^{n-1} F(8r) \zeta^{-xr} \quad (j = 0, 1, \dots, n-1) \quad (17)$$

The assumption $q \equiv 1 \pmod{8}$ implies that $r = 0$ is the only value of r in the summation range $0 \leq r \leq n-1$ for which $8r$ is divisible by $q+1$. Therefore Lemma 1 yields

$$F(8r) = \sum_{k=0}^q b_k \overline{b}_{k+8r} = \begin{cases} q & (r = 0) \\ 0 & (1 \leq r \leq n-1). \end{cases} \quad (18)$$

It follows from (18) that the right member of (17) reduces to g . This completes the proof of Theorem 1.

When $\zeta = 1$ the sums $f(\zeta)$ and $g(\zeta)$ in Theorem 1 may be evaluated separately.

COROLLARY 1. In the case $\zeta = 1$ the identity (11) reduces to the identity $q = c^2 + 2d^2$ where c and d are integers.

Proof. There does not appear to be any straightforward way to derive the corollary from the theorem. It is convenient to put $\theta = \tau^{q-1}$ as in (5). We begin by expressing the sum

$$L(\chi) = \sum_{k=0}^q \chi(\theta^{k+1})$$

in terms of $f(1)$ and $g(1)$. We have

$$\begin{aligned} L(\chi) &= \sum_{j=0}^{n-1} \chi(\theta^{2j+1}) + \sum_{j=0}^{n-1} \chi(\theta^{2j+1+1}) \\ &= \sum_{k=0}^{n-1} \chi(\theta^{8k+1}) + \sum_{k=0}^{n-1} \chi(\theta^{8k+n+1}). \end{aligned}$$

From (5) we obtain $\chi(\theta^{8k+1}) = \chi(2)b_{8k}$ and $\chi(\theta^{8k+n+1}) = \chi(2)\beta^{-n+2}a_{8k}$. Since 2 is the square of an element in $GF(q)$ the value of $\chi(2)$ is ± 1 . The value of $\chi(\theta^{8k+1})$ is an even power of β , and the value of $\chi(\theta^{8k+n+1})$ is an odd power of β . Since $n \equiv 1$ or $5 \pmod{8}$ according as $q \equiv 1$ or $q \pmod{16}$ we deduce

$$L(\chi) = \chi(2)\{g(1) \pm \beta f(1)\}, \quad (19)$$

where the ambiguous sign is plus if $q \equiv 1 \pmod{16}$ and minus if $q \equiv 9 \pmod{16}$.

We next transform $L(\chi)$ into the Eisenstein sum

$$E(\chi) = \sum_b \chi(1+b\gamma),$$

where b runs over the elements of $GF(q)$.

We follow the method of P.A. Leonard and K.S. Williams [7; p. 306].

For $b \in GF(q)$ the elements $(1-b\gamma)/(1+b\gamma)$ are distinct and different from -1 , as $((1-b\gamma)/(1+b\gamma))^q = (1+b\gamma)/(1-b\gamma)$, each of them satisfies $y^{q+1} = 1$, and so these q elements of $GF(q^2)$ are simply θ^k , $1 \leq k \leq q+1$, $k \neq (q+1)/2$. Therefore

$$\{\theta^{k+1} \mid 1 \leq k \leq q+1, k \neq \frac{q+1}{2}\} = \{ \frac{2}{1+b\gamma} \mid b \in GF(q) \},$$

so that

$$\sum_{k=1}^{q+1} \chi(\theta^{k+1}) = \sum_{k=1}^{q+1} \chi'(\theta^{k+1}) = \sum_b \chi(\frac{2}{1+b\gamma}) = \chi(2) \sum_b \overline{\chi}(1+b\gamma)$$

where the dash (') over the second sum indicates that the value $k = (q+1)/2$ is excluded. We have thus established

$$L(\chi) = \chi(2)E(\overline{\chi}), \quad (20)$$

where $\overline{\chi}$ is the character conjugate to χ .

Comparing (19) and (20) we obtain

$$E(\overline{\chi}) = g(1) \pm \beta f(1). \quad (21)$$

By employing the theory of Jacobi sums Bruce C. Berndt and Ronald J. Evans [3; Chapter 4] have evaluated $E(\chi)$ for q an odd prime power. The following lemma is part of the Theorem 4.1.

LEMMA 2. Let $q \equiv 1 \pmod{8}$, and let χ be a character of $GF(q^2)$ of order 8. Then

$$E(\chi) = c + d\sqrt{-2} \quad (22)$$

where c and d are integers such that $c^2 + 2d^2 = q$ and $c \equiv 1 \pmod{4}$.

Finally we compare (21) and (22). Since $\overline{\chi}$ is a character on $GF(q^2)$ of order 8 we have $E(\chi) = E(\overline{\chi})$. Furthermore, $\beta + \beta^3 = \beta(1+i) = \sqrt{-2}$. Since the terms of $f(1)$ and $g(1)$ are even powers of β it follows that $g(1) = c$ and $f(1) = \pm d(1+i)$. This completes the proof of the corollary.

4. Applications.

Theorem 1 yields the following analogue of a valuable result of Goethals and Seidel [6 or 11, Theorem 3.18].

THEOREM 2. Let $q \equiv 1 \pmod{8}$ be a prime power. Then there exists a square matrix P of order $q+1$ with diagonal elements 0 and all other elements $\pm 1, \pm i$ such that

$$PP^* = qI_{q+1} \quad \text{and} \quad P = \begin{pmatrix} R & S \\ S^* & -R^* \end{pmatrix} \quad (23)$$

where R and S are symmetric circulants. This is a $CW(q+1, q, z_4)$.

Proof. The matrices R and S in Theorem 2 are obtained from the polynomials $f(\zeta)$ and $g(\zeta)$ in Theorem 1. The elements in the top row of the circulant R are the consecutive coefficients $a_0, a_8, \dots, a_{8(n-1)}$ of $f(\zeta)$, and the elements in the top row of the circulant S are the consecutive coefficients $b_0, b_8, \dots, b_{8(n-1)}$ of $g(\zeta)$. The symmetry of R and S is expressed in (13). Since $a_0 = 0$ the diagonal elements in P are all 0. For $n = (q+1)/2$ the matrix equation

$$RR^* + SS^* = qI_n \quad (24)$$

is equivalent to the orthogonality relation

$$\sum_{i=0}^{n-1} (a_{8i} \bar{a}_{8i+8r} + b_{8i} \bar{b}_{8i+8r}) = \begin{cases} q & (r = 0), \\ 0 & (1 \leq r \leq n-1), \end{cases}$$

which follows from (14), (15) and (18). Consequently, (23) may be established by a straightforward verification.

Examples. In the following two examples the top rows of the circulants R and S are given.

$$q = 9: \quad R = (0, 1, 1, 1, i), \quad S = (1, -i, i, i, -i)$$

$$f(1) = 2 + 2i, \quad g(1) = 1$$

$$|f(1)|^2 + |g(1)|^2 = 1^2 + 2 \cdot 2^2 = 9.$$

$$\begin{aligned}
q = 17: \quad R &= (0, i, 1, -i, i, i, -i, 1, i) \\
S &= (1, i, -i, -1, i, -1, -1, -i, i) \\
f(1) &= 2 + 2i, \quad g(1) = -3 \\
|f(1)|^2 + |g(1)|^2 &= (-3)^2 + 2 \cdot 2^2 = 17.
\end{aligned}$$

The following Theorem of Williamson [14, 11 p. 382] as adopted by Geramita, Geramita and Wallis is useful.

LEMMA 3. Suppose there exist four symmetric circulant matrices A, B, C, D of order n which satisfy

$$AA^T + BB^T + CC^T + DD^T = fI_n$$

where f is a quadratic form. Then

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix} \quad (25)$$

satisfies

$$HH^T = fI_{4n}.$$

Hence, if A, B, C, D have entries from the set of commuting variables $\{0, \pm x_1, \pm x_2, \dots\}$, H is an orthogonal design.

We shall now employ Theorem 2 to produce the following family of orthogonal designs and weighing matrices to give insight into the internal structure. It should be noted that there is another proof which follows easily from a theorem of Delsante, Goethals and Seidel.

THEOREM 3. Let $q \equiv 1 \pmod{8}$ be a prime power. Then there exists an orthogonal design of type (q, q) in order $2(q+1)$ as well as a $W(2(q+1), q)$ and a $W(2(q+1), 2q)$.

Proof. Let R and S be the symmetric circulants of Theorem 2. Put $R = U + iV$ and $S = X + iY$. Then we have

$$\begin{aligned}
RR^* + SS^* &= (U + iV)(U - iV) + (X + iY)(X - iY) \\
&= U^2 + V^2 + X^2 + Y^2 + i(VU - UV + YX - XY)
\end{aligned}$$

$$U^2 + V^2 + X^2 + Y^2 = UU^T + VV^T + XX^T + YY^T \quad qI_n$$

in view of (24).

$$\begin{aligned} A^2 + B^2 + C^2 + D^2 &= (x^2 + y^2)(u^2 + v^2 + x^2 + y^2) \\ &= (qx^2 + qy^2)I_m. \end{aligned}$$

Example. In the following two examples (writing $\bar{x} = -x$ and $\bar{y} = -y$) the top rows of the circulants A, B, C, D are given.

$$\begin{array}{ll} q = 9: & A = \{0yxxy\}, \quad B = \{0x\bar{y}\bar{y}x\}, \\ & C = \{x\bar{y}y\bar{y}\}, \quad D = \{y\bar{x}\bar{x}x\}. \\ q = 17: & A = \{0yx\bar{y}y\bar{y}y\bar{y}xy\}, \quad B = \{0x\bar{y}\bar{x}\bar{x}\bar{x}\bar{y}x\} \\ & C = \{x\bar{y}y\bar{x}\bar{x}\bar{x}\bar{y}\bar{y}\}, \quad D = \{\bar{y}\bar{x}\bar{y}y\bar{y}\bar{x}\bar{x}\}. \end{array}$$

THEOREM 4. *Let $q \equiv 1 \pmod{8}$ be a prime power. Then there exists an orthogonal design of type $(4, 2q, 2q)$ in order $4(q+1)$.*

$$\begin{aligned} A &= zI + xU + yV, & B &= -zI + xU + yV, & C &= zI + yU - xV, \\ D &= -zI + yU - xV, & E &= xX + yY, & F &= xX + yY, \\ G &= yX - xY, & H &= yX - xY, \end{aligned}$$

We now derive another result using Theorem 2.

Suppose $z = X+iY$ is a cod. of order m and type (z_1, z_2, \dots, z_r) then $XX^T + YY^T = fI_m$, where f is a quadratic form, and $XY^T = YX^T$.

THEOREM 5. Suppose there exists an orthogonal design of type (a, a) in order n and a cod of order m and type (z_1, z_2, \dots, z_r) . Then there exists an orthogonal design of type $(az_1, az_2, \dots, az_r)$ in order mn .

Proof. Write $z = X+iY$ for the cod. Replace the first and second variables of the orthogonal design $xA_1 + yA_2$ by X and Y respectively to obtain $W = A_1XX + A_2XY$ then

$$\begin{aligned} WW^T &= A_1A_1^TXX^T + A_1A_2^TXXY^T + A_2A_1^TXYX^T + A_2A_2^TXY Y^T \\ &= aI \times (XX^T + YY^T) + (A_1A_2^T + A_2A_1^T) \times XY^T \\ &= afI_{nm}. \end{aligned}$$

Hence W is the required orthogonal design.

Corollary 4.116 of Geramita and Seberry establishes that an orthogonal design of type (r, r) exists in order $2n$, $n \geq 2^a 10^b 26^c 6^d 14^e$ for each r of the form $2^a 10^b 26^c 5^d 13^e$ where a, b, c, d, e are non-negative integers.

COROLLARY 2. Let r and n be as just described. Suppose there exists a complex orthogonal design of type (z_1, z_2, \dots, z_r) in order m . Then there exists an orthogonal design of type $(rz_1, rz_2, \dots, rz_r)$ in order $2mn$.

This corollary is a generalization of Construction 19 of [4] which gives this result for $r = 2$.

Using Theorem 2 with Theorem 5 we have:

COROLLARY 3. Let $q \equiv 1 \pmod{8}$ be a prime power. Let r and n be as described above. Then there exists an orthogonal design of type (rq) in every order $\geq n(q+1)$. Equivalently, there exists a $W(m(q+1), rq)$ for every $m \geq n$.

5. New Cods.

We note in passing that if a, b, c are commuting variables and $i^2 = -1$ then

$$(i) \quad a^2 c - a^2 \quad \text{and} \quad a^2 i b a$$

(ii) $a_1 c_1 a_2 b_1 - a_2$ and $a_1 c_1 a_2 - a_1 b_1$

are sequences with zero-autocorrelation which can be used as first rows of circulant matrices of order $n \geq 3$ and $n \geq 5$ respectively by adding a suitable number of zeros to the end of each sequence and which can be used in Construction 8 of [4] to obtain:

LEMMA 3. *There exist codes of type (1,1,4) in all orders $2n$, $n \geq 3$ and of types (2,2,8), (2,10), (4,8) and (12) in all orders $2n$, $n \geq 5$.*

This gives some unsolved cases of Geramita and Geramita [4].

REFERENCES

- [1] Gerald Berman, *Weighing matrices and group divisible designs determined by $EG(t, p^n)$, $t > 2$* , Utilitas Math. 12 (1977), 183-192.
- [2] Gerald Berman, *Families of generalized weighing matrices*, Canad. J. Math.
- [3] Bruce C. Berndt and Ronald J. Evans, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal and Brewer*, Illinois J. Math.
- [4] A.V. Geramita and Joan M. Geramita, *Complex orthogonal designs*, J. Combinatorial Th. (Ser.A) 25, (1978), 211-225.
- [5] Anthony V. Geramita and Jennifer Seberry, *Orthogonal Designs: Quadratic forms and Hadamard matrices*, Marcel Dekker, New York, 1978.
- [6] J.M. Goethals and J.J. Seidel, *Orthogonal matrices with zero diagonal*, Canad J. Math. 19(1967), 1001-1010.
- [7] Philip A. Leonard and Kenneth S. Williams, *Jacobi sums and a theorem of Brewer*, Rocky Mountain J. Math. 5(1975), 301-308.
- [8] R.C. Mullin and R.G. Stanton, *Group matrices and balanced weighing designs*, Utilitas Math. 8(1975), 277-301.
- [9] R.C. Mullin and R.G. Stanton, *Balanced weighing matrices and group divisible designs*, Utilitas Math. 8(1975), 303-310.
- [10] Jennifer Seberry, *Some remarks on generalized Hadamard matrices and theorems of Rajkondlia on SBIBDs*, Combinatorics VI: Proceedings of the Sixth Australian Conference, Armidale, August, 1978.

- [11] Jennifer Seberry Wallis, *Hadamard matrices, Part III of Combinatorics: Room Squares, sum free sets and Hadamard matrices* by W.D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, in *Lecture Notes in Mathematics*, Vol. 292, Springer-Verlag, Berlin-Heidelberg-New York, 1972, 273-489.
- [12] G.A. Vanstone and R.C. Mullin, *A note on existence of weighing matrices $W(2^{2n-j}, 2^n)$ and associated combinatorial designs*, *Utilitas Math.* 8(1975), 371-381.
- [13] Jennifer Wallis, *Orthogonal $(0,1,-1)$ -matrices*, *Proc. First Australian Conf. on Combinatorial Math.* (ed. Jennifer Wallis and W.D. Wallis) TUNRA, Newcastle, Australia (1972), 61-84.
- [14] John Williamson, *Hadamard's determinant theorem and the sum of four squares*, *Duke Math. J.* (1944), 65-81.

Dept. Applied Mathematics
University of Sydney
N.S.W. 2006

Dept. of Mathematics
University of Southern California
Los Angeles, California